"Mod p" Arithmetic and Algebra.
Topics in Algebra 5900
Spring 2011
Aaron Bertram

Let p be a prime number.

Definition. (i) The "mod p" numbers are all the remainders:

$$\{0, 1, 2, \ldots, p-1\}$$

when a natural number is divided by p.

(ii) Addition and multiplication are defined in two steps:

Step 1. Add (or multiply) two given remainders.

Step 2. Divide the result by p and replace it with the remainder.

Example. In mod 17 arithmetic:

$12 + 13 = 8$ (the remainder when 25 is divided by 17) and

$12 \cdot 13 = 3$ (the remainder when 156 is divided by 17)

Mod p Arithmetic Theorem.

Addition and multiplication of the mod p numbers have all the good properties of the rational numbers. That is:

(a) The commutative, associative and distributive laws all hold.

(b) Every number mod p has an additive inverse (i.e. a "negative").

(c) Every number mod p except zero has a mod p reciprocal.

Tables for Small Values of p.

Here are the addition and multiplication tables **mod 2**:

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

This includes one peculiar equation:

$$1 + 1 = 0 \pmod 2$$

from which it follows that:

$$-1 = 1 \pmod 2$$

This will take some getting used to, but remember that the *meaning* of -1 is "the number you add to 1 to get 0."

And here are the addition and multiplication tables **mod 3**:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Here we have two peculiar equations:

$$1 + 2 = 0 \text{ (mod 3) and } 2 \cdot 2 = 1 \text{ mod 3}$$

which give us two additive inverses and one reciprocal:

$$-1 = 2 \text{ (mod 3)}, \quad -2 = 1 \text{ (mod 3)} \quad \text{and} \quad 1/2 = 2 \text{ (mod 3)}$$

remembering that $1/2$ *is* the number you multiply by 2 to get 1.

It is worth repeating the remarkable feature of mod p arithmetic. When doing arithmetic mod p, we do not need to introduce fractions in order to find reciprocals. Reciprocals of mod p numbers are other mod p numbers!

Another Set of Tables: The tables for **mod 5** arithmetic are:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverses in mod 5 arithmetic:

$$-1 = 4, \ -2 = 3, \ -3 = 2, -4 = 1 \text{ (mod 5) and}$$

$$1/2 = 3, \ 1/3 = 2 \text{ and } 1/4 = 4 \text{ (mod 5)}$$

Some patterns are now emerging. First,

Additive inverses mod p are easy to find. Since:

$$k + (p - k) = p \text{ for all } k = 0, 1, \ldots, p - 1$$

it follows that k and $p - k$ are additive inverses of each other. That is:

$$-k = p - k \text{ (mod } p)$$

This means, for example, that we can replace $p - k$ with $-k$ in the multiplication tables and cut the work in half. The addition tables by now are easy to fill in. We'll concentrate on multiplication tables for the next two primes, and leave out the row and column of zeroes.

Three More Primes: The multiplication table **mod 7** is:

*	1	2	3	-3	-2	-1
1	1	2	3	-3	-2	-1
2	2	-3	-1	1	3	-2
3	3	-1	2	-2	1	-3
-3	-3	1	-2	2	-1	3
-2	-2	3	1	-1	-3	2
-1	-1	-2	-3	3	2	1

The reciprocal "table" is:

$1/2 = -3,\ 1/3 = -2,\ 1/(-3) = 2,\ 1/(-2) = 3,\ 1/(-1) = -1 \pmod 7$

The multiplication table **mod 11** is:

*	1	2	3	4	5	-5	-4	-3	-2	-1
1	1	2	3	4	5	-5	-4	-3	-2	-1
2	2	4	-5	-3	-1	1	3	5	-4	-2
3	3	-5	-2	1	4	-4	-1	2	5	-3
4	4	-3	1	5	-2	2	-5	-1	3	-4
5	5	-1	4	-2	3	-3	2	-4	1	-5
-5	-5	1	-4	2	-3	3	-2	4	-1	5
-4	-4	3	-1	-5	2	-2	5	1	-3	4
-3	-3	5	2	-1	-4	4	1	-2	-5	3
-2	-2	-4	5	3	1	-1	-3	-5	4	2
-1	-1	-2	-3	-4	-5	5	4	3	2	1

We can really reduce the size of these tables if we use the rules for multiplication by additive inverses:

$$(-a)b = a(-b) = -ab \text{ and } (-a)(-b) = ab$$

so we only have to record the products of "positive" numbers mod p.

The streamlined multiplication table **mod 13** is:

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	-5	-3	-1
3	3	6	-4	-1	2	5
4	4	-5	-1	3	-6	-2
5	5	-3	2	-6	-1	4
6	6	-1	5	-2	4	-3

and the reciprocal table is:

$1/1 = 1,\ 1/2 = -6,\ 1/3 = -4,\ 1/4 = -3,\ 1/5 = -5,\ 1/6 = -2 \pmod{13}$

One Last Table: Using the commutative law of multiplication, we can even cut the streamlined table (almost) in half, since we don't need the lower left triangle. With this in mind, the super-streamlined multiplication table **mod 17** is:

*	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2		4	6	8	-7	-5	-3	-1
3			-8	-5	-2	1	4	7
4				-1	3	7	-6	-2
5					8	-4	1	6
6						2	8	-3
7							-2	5
8								-4

Exercise 1. Work out the super-streamlined multiplication tables:

(a) mod 19

(b) mod 23

(c) mod 29

Mod p Algebra Theorem.

Equations involving variables are solved "mod p" just as they are solved in ordinary algebra, keeping in mind that:

(a) All constants are mod p numbers.

(b) All arithmetic is mod p arithmetic.

(c) All variables stand for mod p numbers.

Linear Equations mod p are equations of the form:

$$ax + b = c \pmod{\text{p}}$$

They are solved exactly as usual. Namely:

Step 1. Subtract b from both sides (mod p).

Step 2. Multiply both sides by the reciprocal of a to solve:

$$x = \frac{c - b}{a} \pmod{\text{p}}$$

Example. Solve:

$$3x + 4 = 1 \pmod{5}$$

Step 1. Subtract 4 from both sides.

Since $-4 = 1 \pmod 5$ this is the same as adding 1 to both sides!

$$3x = (1 - 4) = (1 + 1) = 2 \pmod 5$$

Step 2. Divide both sides by 3.

Since $1/3 = 2 \pmod 5$, this is the same as multiplying both sides by 2.

$$x = \frac{2}{3} = 2 \cdot \frac{1}{3} = 2 \cdot 2 = 4 \pmod 5$$

Let's check the result. Setting $x = 4 \pmod 5$ gives us:

$$3x + 4 = 3 \cdot 4 + 4 = 2 + 4 = 1 \pmod 5 \quad \text{Check!}$$

Another Example. Solve the same equation mod 7:

$$3x + 4 = 1 \pmod 7$$

Step 1. Use $-4 = 3 \pmod 7$ to subtract 4 from both sides:

$$3x = (1 - 4) = (1 + 3) = 4 \pmod 7$$

Step 2. Use $1/3 = 5$ mod 7 to divide both sides by 3:

$$x = 4/3 = 4 \cdot 5 = 6 \pmod 7$$

Now check: $3 \cdot 6 + 4 = 4 + 4 = 1 \pmod 7$. Check!

Standard Quadratic Equations are of the form:

$$ax^2 + bx + c = 0 \pmod{\text{p}}$$

We want to solve them as usual by *completing the square.*

Step 1. Subtract c from both sides:

$$ax^2 + bx = -c \pmod{\text{p}}$$

Step 2. Multiply both sides by $4a$:

$$4a^2x^2 + 4ab = -4ac \pmod{\text{p}}$$

Step 3. Add b^2 to both sides.

$$4a^2x^2 + 4ab + b^2 = b^2 - 4ac \pmod{\text{p}}$$

Step 4. Factor the left side:

$$(2ax + b)^2 = b^2 - 4ac \pmod{\text{p}}$$

Step 5. Take square roots of both sides:

$$2ax + b = \pm\sqrt{b^2 - 4ac} \pmod{\text{p}}$$

Step 6. Subtract b from both sides and divide by $2a$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \text{ (mod p)}$$

Voila! The quadratic formula.

Every step works just as usual except we have the following:

Question. How do we take square roots mod p?

The answer is interesting and difficult. It turns out that **half** of the numbers from 1 to $p-1$ have square roots, and the other half do not. We can see this for small p by inspection of the multiplication tables.

Squares mod p: For the first few odd primes:

(mod 3) $\pm\sqrt{1} = \pm 1$ but 2 has no square root.

(mod 5) $\pm\sqrt{1} = \pm 1$ and $\pm\sqrt{4} = \pm 2$ but $2, 3$ have no square roots.

(mod 7) $\pm\sqrt{1} = \pm 1$ and $\pm\sqrt{4} = \pm 2$ and $\pm\sqrt{2} = \pm 3$
The other numbers: $3, 5, 6$ have no square roots.

(mod 11) $\pm\sqrt{1} = \pm 1, \pm\sqrt{4} = \pm 2, \pm\sqrt{9} = \pm 3, \pm\sqrt{5} = \pm 4, \pm\sqrt{3} = \pm 5$.
The other numbers: $2, 6, 7, 8, 10$ have no square roots.

Exercise 2. Continue this for the primes $p = 13, 17, 19, 23$ and 29.

Remember that with the real numbers, the *discriminant*

$$b^2 - 4ac$$

has two square roots if it is positive and none if it is negative.

Unfortunately, in mod p algebra, we have nothing like the sign of the discriminant to guide us to whether or not $b^2 - 4ac$ has a square root mod p. There is an amazing result, known as *Quadratic Reciprocity*, that helps us tell whether numbers have square roots mod p, but this would take us too far afield. We will just be satisified here with seeing what happens one prime at a time.

Example: In ordinary algebra, the two solutions to:

$$x^2 - x - 1 = 0$$

are the the *golden mean* and its cousin, little golden mean:

$$\phi = \frac{1 \pm \sqrt{5}}{2}$$

What are the mod p solutions for small primes?

(mod 2) This makes no sense mod 2, since we would divide by zero!

(mod 3) $5 = 2 \text{ (mod 3)}$ has no square root, so there are no solutions!

(mod 5) $5 = 0 \pmod 5$ and $\sqrt{0} = 0$, so there is one solution:

$$x = 1/2 = 3 \pmod 5$$

and $3^2 - 3 - 1 = 0 \pmod 5$. Check!

(mod 7) 5 has no square root mod 7, so there are no solutions.

(mod 11) $\pm\sqrt{5} = \pm 4 \pmod{11}$, so there are two solutions:

$$x = \frac{1 \pm 4}{2} = \frac{5}{2} \text{ or } \frac{-3}{2} \pmod{11}$$

and since $1/2 = 6 \pmod{11}$, we finally get:

$$x = 5 \cdot 6 = 8 \text{ or } x = (-3) \cdot 6 = 4 \pmod{11}$$

and $8^2 - 8 - 1 = 55 = 0 \pmod{11}$ and $4^2 - 4 - 1 = 11 = 0 \pmod{11}$. Check!!

Exercise 3. Try this out with more primes, and also find solutions to:

$$x^2 + x + 1 = 0 \text{ (mod p)}$$

for a few primes. (This one has no real solutions, since $b^2 - 4ac = -3$).

Finally, here is something that has no analogue in "ordinary" algebra.

Primitive Numbers mod p

Take a nonzero number mod p and call it a, and consider its powers:

$$a, a^2, a^3, a^4, \ldots \text{ (mod p)}$$

Eventually, you will always get back to 1. In fact:

Fermat's Little Theorem: No matter what $a \neq 0$ you choose,

$$a^{p-1} = 1 \text{ (mod p)}$$

Definition. The number a is *primitive* if the $p-1$st power is the **first** power that gets back to 1.

Examples: Consider the powers of the numbers mod 7:

$$1$$

$$2, 4, 1$$

$$3, 2, 6, 4, 5, 1$$

$$4, 2, 1$$

$$5, 4, 6, 2, 3, 1$$

$$6, 1$$

so 3 and 5 are primitive but the others are not.

It is a fact that primitive numbers mod p exist for any prime p, but it is not such an easy task to find them!

Exercise 4. Find all the primitive numbers:

(a) mod 11

(b) mod 13

(c) mod 17